SOCIAL MEDIA: THE SURFACE DARK WEB

In recent years, the social media has become the common hunting grounds for all hackers/criminals which can affect to a national level or just to seek revenge to an individual. Pentagon officials are increasingly worried that state-backed hackers/criminals are using social media platforms such as Twitter and Facebook to break into computer networks of high ranked or individuals. Therefore exercising such power comes at a high stake.

The human zero-day exploit:

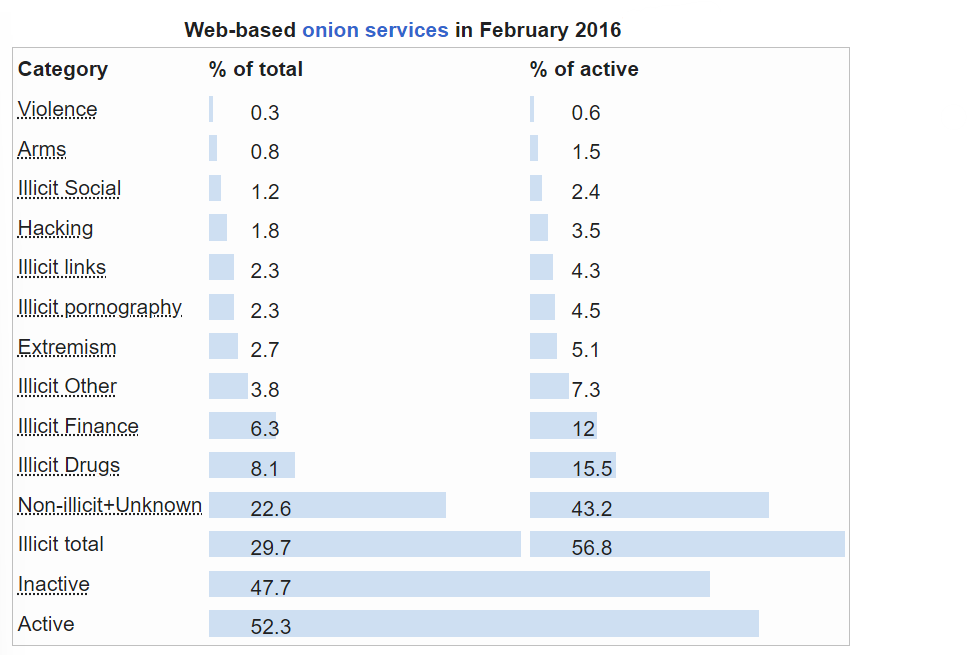
Every Human is vulnerable to being exploited by different methods of which the most common is the *SOCIAL ENGINEERING* or driven by a human error. Withthe variety of social media platforms we commonly use, there are a variety of entry points for hackers/criminals to enter your systems through. We will see some common rather well-known methods of [OSINT](https://osintframework.com/)( Open Source Intelligence Gathering)-

* Social Engineering
* Phishing links
* Convincing emails

Note: Direct approach to the victim\*\*

Dark Web OSINT:

The [Dark Web](https://en.wikipedia.org/wiki/Dark_web) can be accessed using TOR( The Onion Router) which provides a high degree of anonymization for traffic across the network. *Information can be gathered from complex supply chains across dark web markets, forums and illicit communities.*



External attack surface vectors and OSINT:

Conducting OSINT on attack surface can provide invaluable insights of opportunities to know more about the victim.

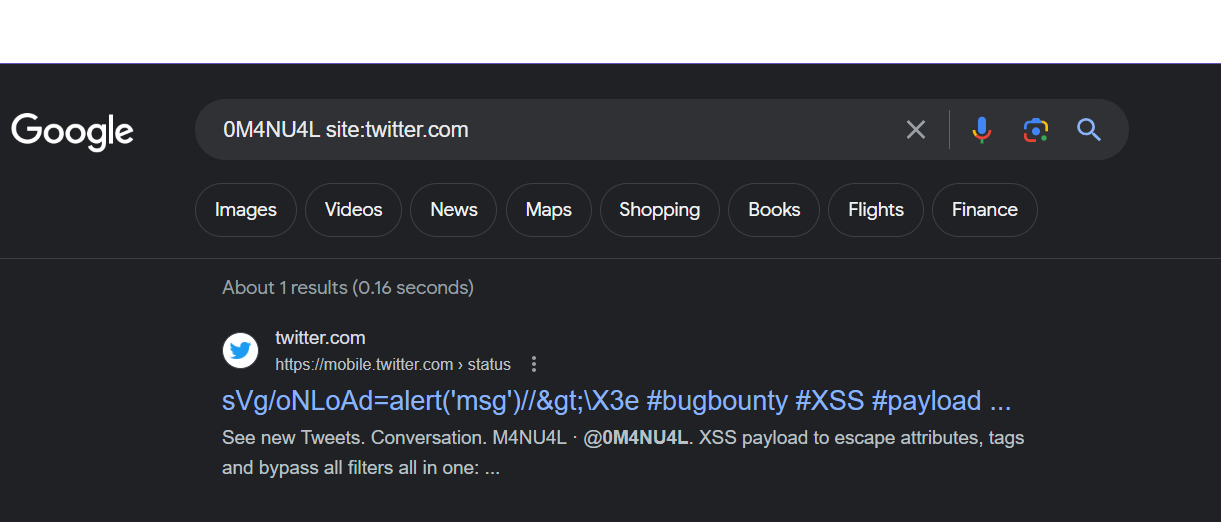
It can lead to sensitive data’s such as:

* Corporate/individual social media profiles
* Business directories
* Phone records
* Victims email
* Location( Real- time)
* Passwords( If leaked)

Google Dorking on Targets:

[Google Dorks](https://en.wikipedia.org/wiki/Google_hacking) are a slightly more advanced method for open source intelligence than collecting relevant news article or social media profile. A *specific search query* is required for dorking.

For example:- intitle:admbook intitle:Fversion filetype:php would locate PHP web pages with the strings “admbook” and “Fversion” in their titles.

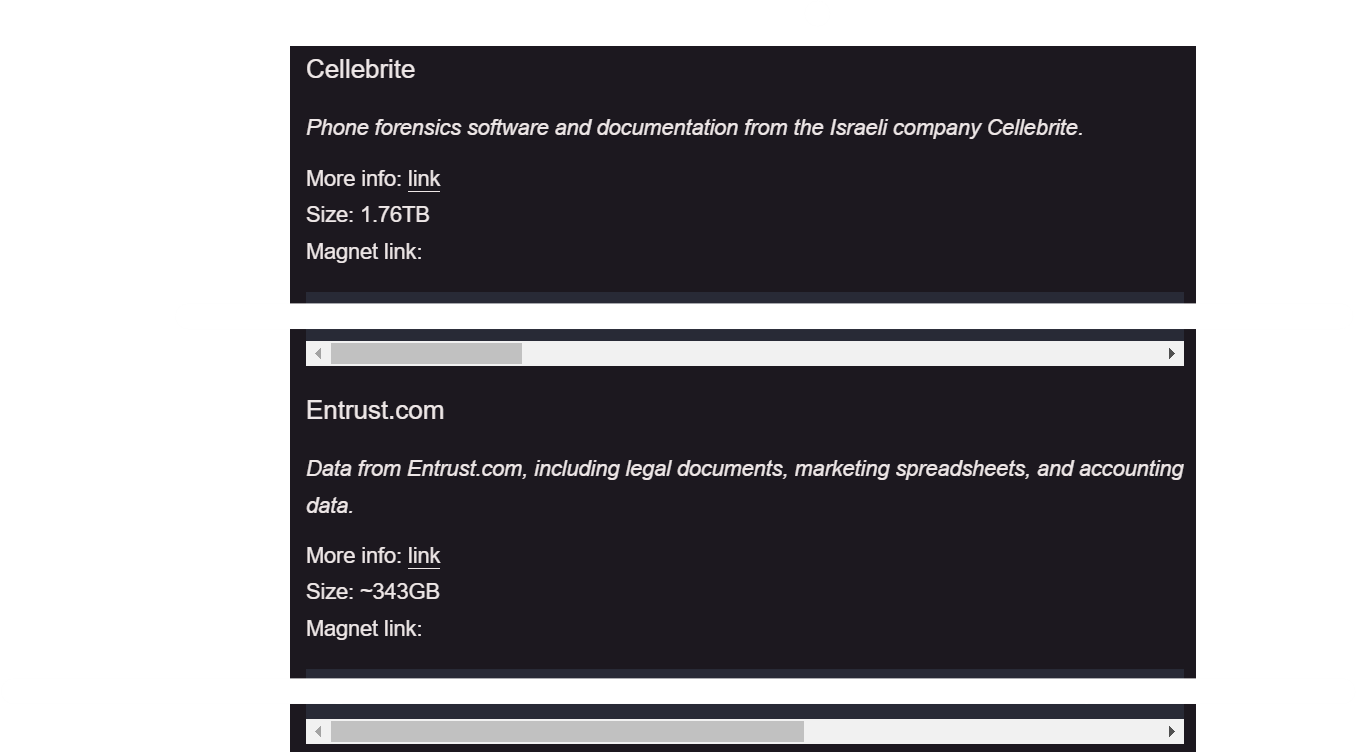


Alt- Locating my twitter handle.

When combined with another dork containing a specific company/individuals name, this would turn up all publicly available data associated with that name/including ones that misconfigured permissions may have inadvertently rendered publicly available.

Data Dumps:

A data dump is usually a large amount of data or files transferred between two systems over a connected network. Therefore it is relatively easier to find people and their email, passwords and sometimes address and credit/debit card information.



Tool:

Tools can be used for extensive research purpose. Listed below are some for their specific use-case:-

* [SEON](https://seon.io/)

Confirming someones identity by checking for linked social media and online platform accounts.

* [EPIEOS](https://epieos.com/)

Allows reverse email/phone search, uses Holehe for precise search operations.

* [Recon-ng](https://www.kali.org/tools/recon-ng/)

Accessible via command-line interface on Kali Linux or as a web application. To assess and identify web vulnerabilities, GeoIP lookup, DNS lookup and port scanning.

* [SpiderFoot](https://www.spiderfoot.net/attack-surface-monitoring/)

Performs regular asset discovery or attack surface monitoring.

* [Have I Been Pwnd](https://haveibeenpwned.com/)

Confirms if your email has been leaked in a email data breach.

* [PhoneInfoga](https://github.com/sundowndev/phoneinfoga)

Open-source tool for OSINT for phone number lookups.

Prevention:

Internet users have used basic cybersecurity measures including antivirus software and a firewall, for a very long time. However, it takes more than that in the age of social media. Setting up serious security measures are required and below are some of them-

* Two-step verification must be used
* Update contact details
* Keep accounts private if age below 18\*\*
* Do not click random links/emails
* Avoid posting/sharing private information
* Avoid leaking email & phone number
* Update the software immediately when rolled

Summary:

Social media platforms have become a hotbed for hacking. However, now that we know that the threats exist and how they happen, we can start protecting ourselves. Clicking on suspicious links and adding people who we do not know is dangerous. However, is the information we often leave out in the open can be equally dangerous. Security starts with being aware and can only evolve with vigilance. Utilizing new tools like two-factor verification will make it harder for hackers to get into your accounts as well.

\*\*EDUCATION PURPOSE BLOG. I WILL NOT BE LIABLE FOR ANY MISUSE\*\*